Government Response to the Intelligence and Security Committee's Annual Report 2010–2011

Presented to Parliament by the Prime Minister
by Command of Her Majesty

October 2011

Cm 8168 £6.00

Any enquiries regarding this publication should be sent to us at committee@isc.x.gsi.gov.uk.

This publication is available for download at www.official-documents.gov.uk and from our website at http://isc.independent.gov.uk.

ISBN: 9780101816823

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2450875 10/11

Printed on paper containing 75% recycled fibre content minimum.

GOVERNMENT RESPONSE TO THE INTELLIGENCE AND SECURITY COMMITTEE'S ANNUAL REPORT 2010–2011

The Government is grateful to the Intelligence and Security Committee (ISC) for providing independent and effective parliamentary oversight of the intelligence and security Agencies and for producing its latest Annual Report.

The ISC's report contains a number of conclusions and recommendations. These are set out below (in **bold**), followed immediately by the Government's response.

A. Given the scale of the spending cuts across government, we recognise that the intelligence and security Agencies received a fair settlement in the Spending Review. Nevertheless, we are concerned that an 11.3% reduction in budgets will inevitably have an impact on the ability of all three Agencies to maintain current levels of coverage of all aspects of the threat, and that this may worsen if inflation remains at its current levels. This will require tough decisions in the coming years.

The Government welcomes the ISC's conclusion that the Single Intelligence Account (SIA) has been given a fair settlement in the Spending Review. This is underlined by the evidence given to the ISC by all three heads of the Agencies. The settlement is sufficient to maintain the range of current operational counter-terrorism capabilities and invest in other key national security objectives such as counter-proliferation. In order to achieve this, the SIA will prioritise spending that delivers front-line capability and increase the pace of saving through collaborative working. This saving will come from making the supporting functions more efficient by delivering more together and also through developing new operational capability that can be used widely across the SIA.

B. Given the importance of national security work, it is essential that the Spending Review settlement can be adjusted if there is a significant change in the threat. The Committee will keep this under review.

The Government agrees with the ISC on the importance of national security work, and the need to ensure that it is adequately funded. As noted above, the Spending Review settlement enables the SIA to maintain counter-terrorism capabilities, where the SIA is already geared to deliver assurance in a high-threat environment, and coverage of the highest priority issues. As noted in the Strategic Defence and Security Review, intelligence capabilities will support the increased emphasis on identifying threats and opportunities early, shaping developments and preventing threats from emerging. The emerging issue of cyber security has its own £650m transformative national programme, much of which will fund SIA activity. Where the changing world environment places new demands on the SIA – as current events in the Middle East may do – the SIA will first look to reprioritise from within its existing work. Agility and flexibility are established strengths of the British intelligence community. The Government will work with the SIA to ensure that the National Security Council's (NSC's) top requirements are given the priority for resources that they need, and that effort is reduced on those issues deemed to be lower priority.

C. GCHQ's Corporate Technical Investment Portfolio (CTIP), of which SIGMOD is part, accounts for a significant proportion of the SIA expenditure. It is a complex set of programmes that encompasses most of GCHQ's work. The Committee has therefore tasked its Investigator to scrutinise CTIP's structure and overarching governance and report to us his findings. This investigation is now under way. We have also asked the National Audit Office to examine specific projects under the SIGMOD banner in due course, to assess the value for money they offer.

Government Communications Headquarters (GCHQ) welcomes the Committee's interest in their Corporate Technical Investment Portfolio and has co-operated fully with the investigation. The Cabinet Office Capability Review in 2009 noted GCHQ's strong track record in ensuring that the programme is well run and delivers on time and to budget.

D. The Committee is disappointed that government departments and agencies do not view investment in Information Assurance as important, and that this has led to GCHQ having to subsidise CESG by several million pounds per year. We are concerned that there appears to have been little progress in achieving a resolution since last year. The Deputy National Security Adviser must prioritise the development of an effective funding model, which should be implemented within the next six months.

The Government welcomes the Committee's recognition of the importance of Information Assurance (IA) across government. IA is fully represented in the work of the Cabinet Office, which co-ordinates work on cyber security. The Government supports fully the Committee's recommendation and the Deputy National Security Adviser will continue to work with the Communications-Electronics Security Group (CESG) to develop a suitable funding model that will ensure the long-term sustainability of their IA work.

E. We are concerned about GCHQ's inability to retain a suitable cadre of internet specialists to respond to the threat. We therefore urge GCHQ to investigate what might be done within existing pay constraints to improve the situation. We also recommend that the Cabinet Office – as lead department for cyber security – considers whether a system of bonuses for specialist skills, such as exists in the United States, should be introduced.

The Government shares the Committee's concerns regarding maintaining a highly skilled cadre of internet security specialists and is taking a number of proactive steps to address the issue.

Policies for the recruitment and retention of specialist staff are the responsibility of individual departments; however, under the National Cyber Security Programme the Government will support individual departments and agencies in developing cyber security training and skills programmes for their staff.

In addition, the Cabinet Office and GCHQ are both supporters of initiatives such as the Cyber Security Challenge, which promotes careers in cyber security via annual competitions and events while providing advice and opportunities to individuals who wish to start a career in the information security field.

Experienced internet specialists are highly prized by both government and industry and GCHQ recognises that it therefore needs to maintain its competitiveness in the market place. It is for this reason that GCHQ already uses a retention payment system which is reviewed from time to time to ensure that it remains competitive. Those bonuses and the unique appeal of the GCHQ mission help to keep leaver rates low, but GCHQ is also considering other measures to attract and retain suitably skilled staff in greater numbers and welcomes the closer involvement of other government departments to help to achieve this.

F. The Committee welcomes the savings that will accrue from the disposal of GCHQ's London office and Oakley site. However, we remain concerned that GCHQ's accommodation strategy has been haphazard in the past and, with the current rationalisation taking place, lacks any flexibility for the future. The GCHQ Board must plan better for the future and develop a sensible long-term strategy for its accommodation requirements.

GCHQ notes the Committee's concerns about its accommodation strategy but believes that its approach has been a pragmatic response to the need to reduce government spending, recent fluctuations in market values of accommodation assets and changes in staff numbers. In conjunction with the two other Agencies, GCHQ is currently developing a strategy to share SIA accommodation, primarily in London, to reduce costs and create greater flexibility.

G. The Committee is concerned that, over a prolonged period, GCHQ has been unable to account for equipment worth up to £1m. Assets must be monitored effectively and controls must be in place to ensure that public money is not wasted. Whilst the majority of the items that could not be traced attracted no security risk, GCHQ has admitted to us that it cannot guarantee that this is the case for 5% (or 450) of these items. Although the Committee has no reason to believe national security has been compromised, the Agencies must do all they can to avoid the loss of potentially sensitive equipment. The public interest requires that GCHQ learns from the repeated mistakes of the past. The Committee expects GCHQ to ensure that the situation does not arise again.

GCHQ notes the Committee's concerns about asset management and record keeping which were identified in the ISC's Annual Report for 2008/09. Since then GCHQ has worked closely with the National Audit Office and industry partners to develop and implement new, more effective processes.

H. The Committee welcomes the improvement by the Security Service in managing 'end-year surges'. However, we urge the Service to implement the recommendation of the National Audit Office to improve their forecasting processes in order to manage expenditure evenly throughout the financial year.

The Government welcomes the Committee's recognition of the progress the Security Service has made in managing 'end-year surges'. The Service's spending profile for 2010/11 showed a distinct improvement in mitigating the end-year surge. The Service is committed to achieving further improvement through stronger forecasting processes, enhanced training for budget managers and strengthened internal accountability.

I. The Security Service has told the Committee that it has been able to respond effectively to the recent increased threat in Northern Ireland. Nevertheless, given the increase in the number of attacks, it is clear that further sustained effort will be required. In the context of declining resources, this will affect the Service's capability in other areas, which is a matter for concern.

The Government shares the Committee's concern about the threat related to Northern Ireland and recognises the need for continuing Security Service effort in this area. As the Committee notes, the Service has responded to the increased threat by augmenting capability on its Northern Ireland-related work. The Service now intends to consolidate this effort, delivering maximum impact from effective tasking, rigorous prioritisation and strong relationships with its main partners (particularly the Police Service of Northern Ireland). The Service has always prioritised its resources to meet the highest threats. It will continue to retain a flexible approach in doing so.

J. The Service is already focused on planning around the 2012 Olympic Games. The Director General has told us that he considers the Service to be well-placed to manage the risks that the Olympics will bring. The Committee is nevertheless concerned that this will inevitably divert resources from the Service's other work during this period, and thus expose the UK to greater risk. The National Security Council must take such steps as are necessary to minimise the risk to the UK.

The Government notes the Committee's concern and recognises the additional challenges the Olympics will present for the Security Service. The Government considers the Service's plans for meeting these challenges to be well developed and the Service's plans remain on track. A wide range of business change is being implemented which will see the Service build further capacity and strengthen the resilience of its processes to help to meet the additional resource pressures that the Olympics are expected to produce. Its response is designed to be scalable and to maximise agility in meeting surge requirements, while continuing to respond to business-as-usual demands so far as possible. This will require rigorous and challenging risk-based prioritisation but the Service starts from a strong position. The precise scale and timing of the additional pressures the Service will face remain difficult to predict with certainty – this will be kept under close review as the Games draw closer.

K. The Committee recognises that the Security Service needs IT specialists in order to deliver its major technology projects. However, spending on consultants and contractors continues to increase at a significant rate. The Service should consider whether collaborative working – with GCHQ in particular – could provide some savings in this area. The Committee will examine the Agencies' use of consultants and contractors in greater detail over the coming year.

The Government welcomes the Committee's recognition that the Security Service needs the support of specialists to help it to deliver the projects which are central to its IT requirements. This is an important part of the Service's workforce model where it would not make commercial sense to employ those specialist skills in-house for the period a project takes to go from conception to delivery. The use of interim specialists and contractors is kept under constant review in order to secure the best value for money. The Committee is right to identify closer collaborative working as a means of making further savings. The latest initiative in this area is that the three Agencies are engaged in setting up a single unified mechanism for hiring interim specialists and contractors. It is envisaged that this will improve value for money. The Government welcomes the Committee's intention to examine the Agencies' use of consultants and contractors in greater detail.

L. This is the fourth consecutive year that SIS has failed to manage its expenditure effectively throughout the year and has seen an 'end-year surge'. The Intelligence and Security Committee has consistently been critical of this, agreeing with the National Audit Office's view that it increases the risk of inefficiency and lack of value for money. The Committee expects SIS, in the current financial climate, to ensure that it manages its budget sensibly in future and will monitor whether this is happening during the current financial year.

The Secret Intelligence Service (SIS) is tackling this issue robustly. Mindful of the ISC's comments on this issue in earlier annual reports, SIS asked the National Audit Office to look out for evidence of poor value in spending late in the financial year 2009/10. None was identified and SIS is confident that good value was achieved for all spending. There was no significant end-year surge during the financial year 2010/11.

M. The Committee welcomes the establishment of the National Security Council. It is important that there is a forum that meets regularly to enable Ministers to take decisions on national security matters and that provides an opportunity for more regular contact between Ministers and the Heads of the Agencies. The NSC must retain its current status and priority.

The Government welcomes the Committee's support for the work of the National Security Council.

N. The Committee welcomes the fact that – through the National Security Strategy – the requirements process which determines the intelligence and security Agencies' allocation of effort is now given greater priority. It will be important, however, to ensure that threats lower down the hierarchy are still given appropriate attention.

In the 2010 National Security Risk Assessment (NSRA), the Government assessed and prioritised all major domestic and overseas national security risks to the UK. The National Security Council used the final NSRA risk matrix and political considerations to arrive at 15 generic priority risk types, and allocated them into three priority risk tiers. The Government shares the Committee's view of the importance of ensuring that threats lower down the hierarchy are still given the appropriate level of attention. The National Security Strategy stressed that the three tiers represent the highest priorities among a broad set of risks, and that all the risks in the NSRA are considered to be significant areas of concern and all require government action to prevent or mitigate them. The NSRA informs the work of all involved in national security, including the Agencies. The National Security Strategy also defines our National Security Tasks and makes it clear that our strategic intelligence capability must support the core military, diplomatic and domestic security and resilience requirements outlined in them.

O. The Committee welcomes the creation of the National Security Adviser post, and the review of the central security and intelligence structures. As part of this review, the different sets of targets, requirements, priorities and objectives that the Agencies are subject to must be reviewed and simplified: there must be one clear tasking process. In particular, it is important that the work of the Joint Intelligence Committee, and the Requirements and Priorities process, is aligned with the strategic direction being set by the National Security Council.

The Government welcomes the Committee's positive response to the creation of the National Security Adviser post.

The review of central security and intelligence structures has been undertaken with an assumption that the National Security Council's priorities should be the lead driver of the Joint Intelligence Committee's agenda. The Requirements and Priorities process clearly should likewise be aligned with the strategic direction being set by the National Security Council. As part of the most recent Requirements and Priorities process, the prioritisation of intelligence collection was agreed directly by Ministers through the National Security Council.

P. The Committee remains concerned about the overlap in remit and potential for duplication of work between the Office for Security and Counter-Terrorism and the National Security Secretariat in the Cabinet Office. Since central structures are currently being examined, we recommend that thought is given to OSCT's future role in the light of that review.

The Office for Security and Counter-Terrorism's (OSCT's) primary responsibilities are to:

- support the Home Secretary and other Ministers by developing, co-ordinating and assessing the impact of CONTEST across Government;
- deliver directly a range of CONTEST programmes (e.g. counter-terrorism related legislation, executive actions, warrantry, PREVENT, personnel protection, aviation security, Chemical, Biological, Radiological and Nuclear programmes, counter-terrorism related science and technology, policy on counter-terrorism policing in England and Wales, and contingency planning for specific terrorist incidents);
- facilitate oversight for the Home Secretary of the Security Service and its operations, and of police counter-terrorism operations;
- co-ordinate counter-terrorism crisis management;
- manage the Communications Capability Programme;
- manage the Olympic and Paralympic Games Safety and Security Programme; and
- maintain a dialogue and co-operation with counterparts overseas necessary to achieve OSCT objectives.

The National Security Secretariat (NSS) is not responsible for the activities listed above and there is little overlap between the NSS and OSCT. But the NSS and OSCT do work closely together.

The NSS provides support to the National Security Adviser by co-ordinating the development and implementation of policy for decision-making at the National Security Council. The Secretariat is also responsible for providing policy advice to the Prime Minister, the Deputy Prime Minister and Cabinet Office Ministers on national security and foreign policy matters. It has a wide range of other functions, including the co-ordination of the Government's response during civil emergencies and international crises and overseeing the SIA and the delivery of the Government's Cyber Security Programme. The Secretariat has also delivered a number of cross-departmental projects, including the National Security Strategy and Strategic Defence and Security Review.

Q. The Committee accepts that it is not easily achieved, but it is nevertheless essential that there is some mechanism by which the success of work on the PREVENT strand of CONTEST – and the benefits of RICU in particular – can be evaluated.

The need for better evaluation of PREVENT work was identified by the Government in its recent review of PREVENT. OSCT is currently working to improve the performance monitoring and evaluation of CONTEST as a whole and PREVENT in particular. PREVENT funding will be rigorously assessed against sound business case criteria to ensure alignment to the new strategy, consideration of benefits, value for money and risk. The aim is to ensure that PREVENT projects are more likely to reach people who are vulnerable to radicalisation.

PREVENT performance indicators are under development and are listed in the new CONTEST strategy: 1) public support in the UK and overseas for terrorism; 2) the proportion of the 25 priority local areas in which implementation of the PREVENT programme is on track; 3) the numbers participating in PREVENT programmes to support vulnerable people, and the proportion assessed to be at lower risk of supporting or engaging in terrorism-related activity after completing the programme; 4) popularity of terrorism-related websites and the impact of our work to disrupt terrorist content; and 5) the extent of radicalisation in prisons. These indicators may change slightly in their final form, depending in particular on whether we are satisfied that supporting data will be available.

The Government is committed to developing more professional counter-narrative products. The Research, Information and Communications Unit (RICU) will focus on the priority geographical areas and sectors identified in the new PREVENT strategy. Its output and impact will be regularly assessed and reported to Ministers in the Home Office and Foreign and Commonwealth Office.

R. The Committee notes the assurance provided by the Director General of the Security Service that, with additional funding and the measures included in the Terrorism Prevention and Investigation Measures Bill, there should be no substantial increase in overall risk. However, any increase at all in the overall threat to national security would be a matter of serious concern. The Committee will take further evidence on the impact of the new regime in due course.

The Government notes the Committee's comments and its intention to take further evidence on the impact of the new regime in due course.

Protecting the public will always be the Government's highest priority. The Government considers that the Terrorism Prevention and Investigation Measures Bill provides robust and effective powers for dealing with the risk posed by suspected terrorists who we can neither prosecute nor deport. These measures will be complemented by significantly increased funding to create additional police and Security Service capabilities for covert surveillance and investigation. These capabilities may additionally increase the opportunities for the collection of evidence which may be used in a prosecution. The Government has also made clear that it will prepare draft emergency legislation for

introduction if, in exceptional circumstances, more stringent measures are required to protect the public. The emergency Bill will be made available for pre-legislative scrutiny.

S. Counter-Terrorism work must be effectively co-ordinated and there must be a clear strategy. Work falling under CONTEST has been subject to a number of separate reviews over the last year. The Government must ensure that these do not operate in isolation from each other and that the end result is properly co-ordinated.

The Government notes the ISC's recommendation and agrees the need for a clear strategy and effective co-ordination of counter-terrorism work. The UK has a comprehensive strategy for countering terrorism: CONTEST. A revised version of CONTEST was published in July 2011.

The latest edition of CONTEST incorporates recommendations from all the reviews of counter-terrorism policy conducted by the Government and draws them together into a coherent whole. CONTEST sets out our overall aim, objectives and vision of success, together with our planning assumptions regarding the terrorist threat for 2011–15.

T. It is disappointing that the Strategic Tasking Directive did not prove a satisfactory system for setting Defence Intelligence's priorities. In devising a new process, Defence Intelligence must take account of the results of the review of central intelligence structures and strategies, and the implications of that review for the setting of national priorities and tasking of the intelligence community.

Defence Intelligence remains committed to providing strategic intelligence to inform Ministry of Defence and other government customers in line with both national and defence priorities.

U. The Committee welcomes the fact that Defence Intelligence is recruiting additional staff to expand its HUMINT capability, which is vital to counter the threat to our Armed Forces from Improvised Explosive Devices in particular. However, the Committee is concerned that the shortage of HUMINT instructors means that these new recruits cannot be deployed quickly. It is also concerning that existing HUMINT operators, who were already under pressure covering vacancies in theatre, are now being placed under further pressure by having to train the new recruits.

The Government is fully committed to the safety and welfare of Armed Forces personnel engaged in operations, ensuring that they receive adequate rest and recuperation following operational deployments, and also places great importance on the training they receive. Using individuals who have recently returned from operational tours in the training environment ensures that up-to-date operational experience and knowledge are passed on to trainees. This support to the training establishment has increased the pass rate, which in turn assists with meeting operational requirements.

V. Defence Intelligence provides the largest single all-source assessment capability within the UK intelligence community. The ISC has, since 2008, consistently raised concerns about the diminution of its coverage and capability. The prospect of further cuts – combined with the impact of cuts to BBC Monitoring, on which DI relies heavily – therefore has potentially very serious long-term consequences for DI's ability to support military operations and for the UK intelligence community as a whole.

The Government welcomes the Committee's recognition of the contribution of Defence Intelligence in support of military operations and to the wider intelligence community. Consultation with Defence Intelligence customers, along with careful prioritisation of analytical effort, remains key to ensuring that Defence Intelligence continues to respond to priority requirements and maintains capability for the longer term. The Government is working with BBC Monitoring to examine requirements and levels of support in order to ensure that they continue to provide adequate levels of service after transition to BBC main.

W. The Committee welcomes the identification of cyber security as a Tier One risk in the National Security Strategy and the increased investment in this crucial area. However, concerns expressed in the ISC's last Annual Report concerning the lack of clear lines of responsibility and the potential risk of duplication of effort remain. The interests of national security demand that there should be clear lines of Ministerial accountability. We expressed concern that the original system was neither sensible nor appropriate. We strongly support the Government's decision to move Ministerial responsibility to the Cabinet Office.

The Committee is right to identify that cyber security is a holistic challenge which encompasses a number of government departments working together in a co-ordinated effort. The creation of the Office of Cyber Security and Information Assurance (OCSIA) within the Cabinet Office has been designed to co-ordinate and harmonise this cross-government effort. Responsibility for delivering the National Cyber Security Programme and overall accountability for the UK Cyber Security Strategy rest with OCSIA. As the Committee has already recognised, overarching Ministerial responsibility for cyber security now rests with the Minister for the Cabinet Office.

X. The Government's decision to settle claims by former Guantánamo Bay detainees was unpalatable to many. Nevertheless, in the circumstances it was the most sensible course of action. The resources required to defend these claims would have been substantially greater than the cost of the settlement, but more importantly the damage that would have been done to foreign liaison relationships would have left the UK vulnerable. We therefore conclude that it was overwhelmingly in the public interest that the cases were settled out of court. We note that the Government continues to engage with US authorities to secure the release of Shaker Aamer, the last remaining former UK resident in Guantánamo Bay.

The Government is grateful to the Committee for its recognition that settlement of the Guantánamo civil damages cases was overwhelmingly in the public interest for the reasons stated. Settlement of the Guantánamo civil damages cases was an integral element of the package of measures that included an inquiry, publication of the Consolidated Guidance, and a Green Paper on justice and security, announced by the Prime Minister in July 2010 to draw a line under these issues. The Government stands firmly against torture and cruel, inhumane and degrading treatment or punishment wherever it occurs in the world.

Y. The Committee welcomes the publication of the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*. It is essential that the Government's overarching policy in relation to detainees, upon which the lower-level practical guidance used by the Agencies is based, is set out clearly and unambiguously.

The Government welcomes the Committee's comments about the publication of the Consolidated Guidance. The Guidance is for personnel operating in the most challenging environments to keep us safe. It is a clear, comprehensive and practical framework for the range of circumstances in which personnel might have involvement with a detainee. It makes plain that we act in compliance with our domestic and international legal obligations and our values as a nation.

Z. **Whilst the previous Committee's *Review of the Government's draft guidance on handling detainees* has not been published, we note that the recommendations and conclusions made by the Committee in the last Parliament were taken into account by the current Government in considering the guidance and have been – to some extent – reflected in the final version now published by the Prime Minister.**

The Government notes the Committee's comments and is grateful to the previous Committee for its input.

AA. We agree with the Government that the Court of Appeal's decision in the Binyam Mohamed case, which resulted in a breach of the 'control principle', has raised serious concerns which need to be resolved urgently. We therefore welcome the Prime Minister's announcement of a Green Paper setting out how intelligence material might be protected in judicial proceedings. The Committee will respond to those proposals in due course.

The Government is committed to producing a Green Paper on justice and security. This will cover the handling of domestic and foreign intelligence material in civil judicial proceedings. We plan to publish in October. We welcome the Committee's intention to respond in due course.

BB. The Committee notes the Coroner's verdicts in the 7/7 Inquests, in particular that – as the ISC itself concluded in its 2009 Report – the Security Service and the police could not reasonably have prevented the attacks. The Committee supports the Coroner's recommendations that the Security Service should improve procedures for showing photographs to sources and that consideration be given to improving the recording of decision-making in relation to the assessment of targets. We have asked the Security Service to report to the Committee on plans to address these matters and will report the progress made in our next Annual Report.

The Government's full response to the Coroner's recommendations was published on 19 July 2011. The Home Secretary and the Director General of the Security Service accepted the two recommendations made in relation to preventability. The response details the improvements made by the Security Service since 2004 in these areas and sets out the further actions planned. The Government welcomes the Committee's intention to keep these matters under review.

CC. We have identified eight examples where there were very minor inaccuracies or inconsistencies in evidence given to the ISC, compared with evidence subsequently provided to the Coroner. We have also identified three discrepancies which are more significant. These are extremely frustrating for the Committee, and for those who rely on our reports. We have satisfied ourselves, however, that they do not alter the conclusions and recommendations that were made in the Committee's *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*.

The Government recognises the Committee's frustration and notes its view that, despite the errors identified in the evidence, the conclusions of the Committee's earlier review remain sound. The Government and the Security Service take seriously matters of factual accuracy in the evidence provided to the ISC. It is therefore a matter of regret that inadvertent errors were present in the evidence provided. The Government and the Security Service recognise the serious impact of such mistakes, whatever their overall substance. As set out in the Government's response to the Coroner's report, the Security Service is confident that improvements in information handling and processing capability have reduced the risk of such errors occurring in similar ISC investigations in future.

DD. The Coroner in the 7/7 Inquests acknowledged that the ISC's second report on the 7 July 2005 terrorist attacks was "*detailed and thorough*". However, she also noted the discrepancies between evidence to the ISC and that given to the Inquests, and criticised the Security Service for their poor record keeping. We share her concerns, having previously made the same point ourselves to the Agencies and to the two previous Prime Ministers. It is essential that the intelligence community make greater efforts to ensure that information provided to this Committee is full and accurate, that searches in response to Committee requests receive the same attention as requests from the courts, and that draft reports are reviewed properly, to ensure that such problems do not arise again.

The Government addressed the Coroner's concerns on the accuracy of evidence provided to the ISC in its response to her Rule 43 Report, published on 19 July 2011.

The Government recognises the importance of the Agencies providing full and accurate information to the Committee. The Agencies are committed to working with the ISC to ensure that relevant information is placed at the Committee's disposal and that such information is accurate. The Government has acknowledged the importance of a rigorous process for checking of factual accuracy.

EE. BBC Monitoring provides an irreplaceable service to the intelligence community, and offers considerable value for money due to the free flow of information with its far larger US counterpart. It is therefore of considerable concern to the Committee that its funding was arbitrarily cut without consultation in April 2010, in direct contravention of the governing Memorandum of Understanding, and that it now faces further cuts over the next two years. The Foreign Affairs Committee has already recommended revisiting the decision about the BBC World Service's funding, and we note the Government's decision to allocate an extra £2.2m to maintain Arabic services. There is also a powerful case for reviewing the decisions that were made about BBC Monitoring's funding in the 2010 Spending Review. The National Security Adviser must ensure that BBC Monitoring is able to maintain the level of service required by departments and Agencies. We strongly recommend that Ministers reconsider the cuts to BBC Monitoring in the period leading up to the transfer to licence fee funding.

The Government welcomes the report's focus on BBC Monitoring (BBCM). The Committee has rightly identified and highlighted the important role that BBCM plays in helping to secure the UK's national security both at home and abroad. BBCM's funding comes from the Cabinet Office. The 2010 cuts highlighted by the Committee were fully in line with those of the wider Cabinet Office and were discussed with BBCM in principle before the start of the financial year. Government stakeholders have worked closely with BBCM (and continue to do so) to identify ways of minimising the impact of reduced funding on this capability.

Interim funding has been agreed with BBCM, and the focus is now on the future and how BBCM will continue to provide its service to the national security community once it is fully integrated into the BBC family. Cabinet Office officials are currently working, on behalf of the National Security Adviser, with stakeholders, the BBC and BBCM to agree the formal and structural arrangements for BBCM both during the transition period and after BBCM has joined BBC main in April 2013. The licence fee agreement places an obligation to provide adequate levels of service.

FF. The Committee welcomes the greater emphasis now being put on collaborative working, both in terms of operational work and corporate services: the Agencies must explore all opportunities to make savings if they are to safeguard their core capability. They have made a good start and we encourage them to maintain this momentum.

The Government fully concurs with the Committee on the importance of Agencies maintaining the momentum on operational and corporate collaboration. This will ensure that the financial, business and operational advantages of collaboration will continue to be generated. In particular, the financial benefits of collaboration in the areas identified by the Director of Collaborative Working, and set out in the ISC's report, are key to maintaining intelligence capabilities in a difficult fiscal environment. Delivering more of the supporting functions together will ensure that the SIA can play its part in deficit reduction while prioritising resources to front-line capabilities.

GG. Although GCHQ has taken steps to reduce its vulnerability to disruptive events – for example through the planned closure of the less-resilient Oakley site – the Committee is very concerned that the lack of a back-up data centre leaves GCHQ exposed should its primary site be out of action. GCHQ should therefore bring forward specific proposals to address this risk at the earliest opportunity.

GCHQ recognises the importance of robust business continuity arrangements and, in particular, the need to deploy operational equipment to more than one site. Their business continuity strategy includes having highly resilient network infrastructure and capability at non-HQ sites to ensure that essential functions and critical services are delivered in the event of disruption at Cheltenham.

Alternative options for additional data centre space are under investigation. The development of a future data centre strategy for all three Agencies forms part of the current collaboration work on IT services.

HH. The Committee accepts that there is a strong case for the Agencies to conduct vetting separately from other parts of government. However, there remains no convincing argument as to why each of the Agencies should maintain separate systems. A single organisation conducting vetting on behalf of all three, with the process tailored to each Agency's specific requirement, would offer considerable benefit. We recommend that the Agencies investigate this as both desirable in its own right and as a potential contribution to their savings targets during the 2010 Spending Review period, and await their response.

The Government notes the Committee's conclusion. The three Agencies are committed to shared corporate services, as part of their plans for living within their Spending Review settlements. How vetting should best fit within that shared services model is under active consideration and it is envisaged that a single SIA vetting service will be established. Preparation towards this goal has been in progress since early 2010, and work on standardisation is already well advanced. Any variations across the Agencies are now well understood, all vetting officers have received joint SIA professional training,

collaboration in a number of areas has commenced and staff have been assigned to develop convergence further. The Committee will be updated as planning in this area develops.

II. The Intelligence and Security Committee was established under the Intelligence Services Act 1994, and has now been in existence for over 16 years. We therefore considered that it was right to review whether the structure, remit and powers of the Committee were still sufficient in the context of the current intelligence machinery. It is clear that the current provisions are outdated and that the *status quo* is unsustainable. We have therefore submitted radical proposals for change that will ensure strengthened, more credible oversight of the UK intelligence and security Agencies and provide greater assurance to the public and to Parliament. We recommend that these form the basis for the proposals for reform of the ISC in the forthcoming Green Paper on the handling of intelligence material in judicial proceedings.

JJ. Our proposals to the National Security Council are based on the following key principles:

- **the Intelligence and Security Committee should become a Committee of Parliament, with the necessary safeguards, reporting both to Parliament and the Prime Minister;**
- **the remit of the Committee must reflect the fact that the ISC has for some years taken evidence from, and made recommendations regarding, the wider intelligence community, and not just SIS, GCHQ and the Security Service;**
- **the Committee's remit must reflect the fact that the Committee is not limited to examining policy, administration and finances, but encompasses all the work of the Agencies;**
- **the Committee must have the power to require information to be provided. Any power to withhold information should be held at Secretary of State level, and not by the Heads of the Agencies; and**
- **the Committee should have greater investigative and research resources at its disposal.**

The Government is committed to producing a Green Paper on justice and security. As well as the subject of the handling of intelligence material in civil judicial proceedings, the Green Paper will also cover the oversight of the intelligence and security Agencies and the wider intelligence community. We expect to publish in October.

The ISC plays a crucial role in the oversight of the intelligence and security Agencies. The ISC's proposals for reform of the ISC are a welcome and important contribution to the debate. It would be premature for the Government to comment further on those proposals in advance of publication of the Green Paper.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, telephone, fax and email
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/general enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call: 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: www.bookshop.parliament.uk

TSO@Blackwell and other accredited agents

ISBN 978-0-10-181682-3